HUNTON& WILLIAMS

National Committee on Vital and Health Statistics
United States Department of Health & Human Services

Testimony on

Privacy Issues Associated with the Use of RFID Technology in Health Care Settings

Lisa J. Sotto, Esq.
Partner
Hunton & Williams LLP
200 Park Avenue
43rd Floor
New York, NY 10021
(212) 309-1223
lsotto@hunton.com

January 11, 2005

Lisa J. Sotto
Hunton & Williams LLP
January 11, 2005

My name is Lisa Sotto and I am a partner in the law firm of Hunton & Williams. I head the firm's Regulatory Privacy and Information Management Practice. I also lead privacy projects for the firm's Center for Information Policy Leadership (the "Center"), which is a privacy think tank affiliated with the law firm. The Center brings together business leaders, government officials, consumer advocates and academic experts to provide thought leadership on a variety of information policy topics. Through both the law firm and the Center, I advise chief privacy officers and other senior executives on the development of global information management programs. I have written and spoken extensively on information management issues, with a focus on privacy in the health care arena. My biographical statement is attached.

Thank you for the opportunity to participate in this hearing. I am doing so on my own behalf and my views should neither be attributed to Hunton & Williams nor to any client of the firm.

I. The Need for Public Trust

RFID technology in the health care arena holds enormous promise. If its use becomes widespread, it can lead to greater accuracy and efficiency in treating patients by making medical information immediately accessible to health care providers. Privacy concerns, however, present a significant obstacle to the widespread acceptance of this technology.

The benefits of using RFID in medical settings are achievable only if patients are confident that the data being transmitted will not be misused. The value of RFID in the medical arena can be fully realized only if patients have confidence both in the security of the technology and in the related policy environment.

II. Categories of Potential Harm

For purposes of discussion, I suggest dividing the privacy concerns related to the use of RFID into distinct categories of potential harm. The relevant categories may be broken down as follows: (1) The inappropriate collection of health information through RFID technology; (2) the intentional misuse or unauthorized disclosure of the data by an authorized data holder; (3) the intentional interception of the information and its subsequent misuse by unauthorized parties; and (4) the unauthorized alteration of the data. I will address each of these categories in turn.

1. The inappropriate collection of health information through RFID technology: In non-medical settings, there is widespread concern that RFID chips may be used to collect data surreptitiously. In libraries, for example, RFID chips can be attached to books without the knowledge of individual borrowers, and information about the borrowers can be collected without consent. In the health care context, this issue does not present as significant a concern. RFID devices in medical settings

generally are used only with the individual's knowledge and consent (or that of the individual's legal representative). Furthermore, with respect to the VeriChip (which is considered the most privacy-invasive of the approved RFID medical devices), all data maintained in the database associated with the chip is self-reported.[1] Thus, in the medical context, use of RFID devices is opt-in. Patients affirmatively choose to provide medical information through RFID technology. In addition, again with respect to the VeriChip, no medical data is stored in the chip itself; instead, the information is maintained in a separate database. Therefore, even if an implanted VeriChip were secretly scanned, the information the interloper would receive would be limited to a 16-digit ID number that has meaning only to those with access to the VeriChip database. The chip itself acts only as a unique identifier, not as a transmitter of health information. Thus, the bigger privacy concern with respect to the VeriChip involves unauthorized access to the VeriChip database. Such unauthorized access is a significant threat to individual privacy, particularly when dealing with sensitive health data. But it is not unique to RFID; unauthorized database access is also an issue in many other contexts (such as online banking) and is frequently managed using security tools like encryption or authentication technologies.[2]

2. The intentional misuse or unauthorized disclosure of the data by the authorized data holder: Another potential harm related to RFID devices is that the party to whom a patient granted permission to access the data for authorized purposes may use or disclose it for unauthorized purposes. This is a legitimate and significant concern. But, again, it is not unique to the RFID context. It is an issue we confront daily in connection with the collection and maintenance of data sets. Whether information is recorded on paper or electronically, guarding against its misuse or unauthorized disclosure is a security and organizational oversight issue that must be

[1] See VeriChip Corporation, Process -- How VeriChip Works (2004), at http://www.4verichip.com/process.htm (last visited Jan. 7, 2005). With respect to the SURGICHIP, the patient assists with both the programming and placement of the chip. See SURGICHIP, SURGICHIP -- Information (2004), at http://www.surgichip.com/surgichip.html (last modified Nov. 14, 2004).

[2] Privacy issues involving the inappropriate collection of medical data through RFID devices will become more significant as technological advances enable RFID chips to store and transmit significant amounts of health information. As chips advance to the point at which they are capable of storing more than just ID numbers or limited surgical data, security tools such as data encryption and authentication technologies must be used in the chip to protect the information from interception.

addressed by every entity that is entrusted with personally-identifiable information.

3. The intentional interception of information and its misuse by unauthorized parties: Any intentional and illicit interception of medical data, and its subsequent use for purposes for which it was not intended, is a clear violation of patient privacy. Here again, however, this is not a new privacy risk that has arisen only as a result of the development of RFID technology. The risk of data interception and misuse involves security issues that plague every organization that stores sensitive data. These problems generally are addressed through encryption and authentication technologies. As with any unauthorized interception of data, the solution is better, more secure technology.

4. The unauthorized alteration of medical data: The risk that a patient's medical information may be inappropriately altered poses a serious threat, not only to the patient's privacy rights, but also to the patient's ability to obtain appropriate medical care. Again, as with the other risks discussed above, the risks related to data integrity are not unique to the RFID context. In any situation in which data integrity is an issue, authentication technologies and other safeguards must be used to help ensure that only those who are authorized to amend the data may do so.

III. A Policy Framework

By dividing into bite-size pieces the potential privacy harms associated with RFID technology, we find that these harms, while extremely serious, are not unique to the RFID context. In the privacy arena, we have been discussing these risks for years. The real question is whether the current regulatory environment provides adequate protection against the potential dangers of RFID technology or whether additional protections are needed to make RFID a secure option.

A. Existing Legal Requirements

For most health care providers, HIPAA's Privacy and Security Rules impose strict limits on the use and disclosure of health information.[3] The restrictions apply without regard to how the data was collected (i.e., whether through RFID-related technology or otherwise). For covered entities, and for their business associates who are contractually restricted in their use and disclosure of health data, no additional protections are necessary.

[3] Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. §§ 160, 164 (2004); Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. §§ 160, 162, 164 (2004).

For RFID-related entities that are not covered by HIPAA,[4] other existing laws provide protection against potential risks involving RFID technology. For example, the unauthorized use or disclosure of medical data may be considered a violation of Section 5 of the Federal Trade Commission ("FTC") Act and its state analogs, which prohibit entities from engaging in unfair or deceptive trade practices. The FTC has availed itself of this provision on numerous occasions to prevent privacy abuses. With respect to unauthorized data users who illicitly intercept and exploit medical information obtained through an RFID network, existing law provides the necessary tools to actively combat and deter this illegal behavior. While the threat of hackers and other bad guys will continue to exist, the tools that are currently in place provide a sufficient framework for law enforcement authorities and private sector security experts to combat illegal activities.

B. A Proposed Code of Conduct

In addition to the protections provided by existing law, an industry code of conduct should be developed for entities that maintain or access RFID-related medical data.[5] The Fair Information Practice Principles[6] and HIPAA's Privacy and Security Rules provide excellent guidance in developing such a code of conduct for the secure use of RFID in health care settings. The code of conduct should contain the following principles:

1. Notice: Patients who are "chipped" must receive notice, written in plain language, of the data holder's information practices. This will allow patients to make informed decisions as to their level of participation in an RFID network. At a minimum, the notice

[4] HIPAA's Privacy and Security Rules apply only to certain entities specifically covered by the regulations.

[5] EPCglobal Inc., an organization that is developing industry-driven standards for the Electronic Product Code ("EPC") to support the use of RFID, has created guidelines for use by companies engaged in the large-scale deployment of EPC. The guidelines "are intended to complement compliance with the substantive and comprehensive body of national and international legislation and regulation that deals with consumer protection, consumer privacy and related issues." EPCglobal, Guidelines on EPC for Consumer Products (2003), at http/www.epcglobalinc.org/public_policy/public_policy_guidelines.html (last visited Jan. 7, 2005). The guidelines set forth the following principles: (i) Consumer notice, (ii) consumer choice, (iii) consumer education and (iv) record use, retention and security. Note that these guidelines are not specific to the use of RFID in medical settings.

[6] Federal Trade Commission, Fair Information Practice Principles, at http://www.ftc.gov/reports/privacy3/fairinfo.htm (last visited Jan. 7, 2005).

should clearly identify the entity collecting the data, the uses and disclosures of the data, the type of data collected and the methods by which the data is collected, the security measures used to safeguard the information, and the rights of the patient with respect to the data (e.g., the right to access and amend the data).

2. Consent: Data holders generally must use and disclose health data only in a manner with which the patient has clearly consented. If the data must be disclosed pursuant to legal requirements (e.g., a subpoena), the data holder should seek to ensure that the recipient uses the data only for the narrow purpose for which it was disclosed and appropriately safeguards the information.

3. Access and Amendment: Patients must have the ability to access their RFID-related health information and to challenge the accuracy of the information and correct it if appropriate. In the health care arena, accuracy of medical information is absolutely critical.

4. Data Integrity and Security: Health information collected in connection with RFID technology must be both accurate and secure. Minimum standards must be established to protect against loss and unauthorized alteration, destruction, access, use and disclosure.

5. Data Retention and Chip Deactivation: There must be clear guidance as to how an individual may (i) deactivate an RFID chip employed for medical purposes and (ii) request the destruction of medical data maintained in an RFID chip or RFID-related database. Under most circumstances, data should be retained only for so long as the individual agrees and must be permanently destroyed once the individual has authorized its destruction.

6. Accountability and Enforcement: Strict accountability standards and enforcement and redress mechanisms must be established for all parties that participate in an RFID system. There must be a price to be paid for being the weak link in a security chain.

IV. Conclusion

The privacy harms that may result from RFID abuses are significant. They are not, however, unique to the RFID context. While I believe existing laws are available to address the potential harms, I would nevertheless encourage RFID stakeholders to develop and adopt an industry code of conduct to further protect against harms that might result from the misuse of data. A coordinated approach by all stakeholders would

provide the public with the confidence needed to support the advancement of this beneficial technology.

Thank you again for the opportunity to appear before you today and address these important privacy issues. I would be happy to answer any questions you may have.